

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION
EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété
Intellectuelle
Bureau international



(43) Date de la publication internationale
19 mai 2005 (19.05.2005)

PCT

(10) Numéro de publication internationale
WO 2005/046278 A3

(51) Classification internationale des brevets⁷ : H04Q 7/38

MOBILE AG [CH/CH]; Schwarztorstrasse 61, CH-3050
Berne (CH).

(21) Numéro de la demande internationale :
PCT/EP2004/052773

(72) Inventeurs; et

(22) Date de dépôt international :
3 novembre 2004 (03.11.2004)

(75) Inventeurs/Déposants (pour US seulement) : KSON-
TINI, Rached [CH/CH]; Route Aloys Fauquez 26,
CH-1004 Lausanne (CH). CANTINI, Renato [IT/CH];
Route du Moulin 35, CH-1782 Belfaux (CH).

(25) Langue de dépôt : français

(74) Mandataire : WENGER, Joel; Léman Consulting S.A.,
Route de Clémenty 62, CH-1260 Nyon (CH).

(26) Langue de publication : français

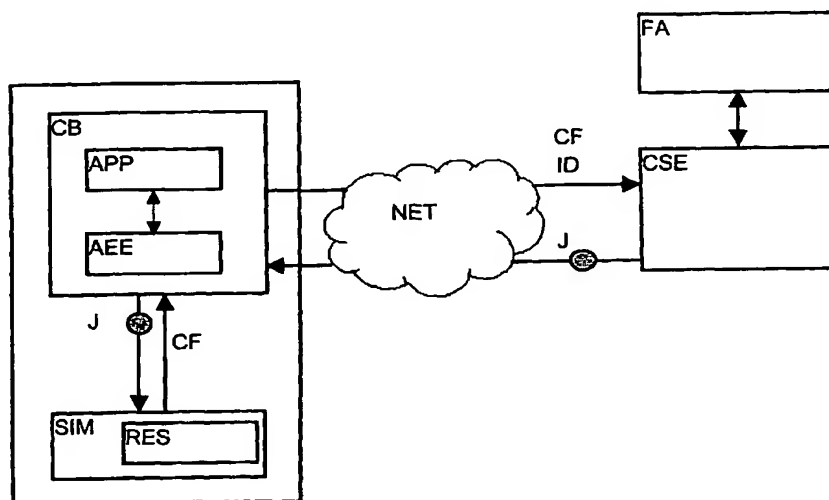
(30) Données relatives à la priorité :
03104069.4 4 novembre 2003 (04.11.2003) EP

(81) États désignés (sauf indication contraire, pour tout titre de
protection nationale disponible) : AE, AG, AL, AM, AT,
AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO,
CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB,
GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG,
KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG,
MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH,

[Suite sur la page suivante]

(54) Title: METHOD FOR MANAGING THE SECURITY OF APPLICATIONS WITH A SECURITY MODULE

(54) Titre : MÉTHODE DE GESTION DE LA SÉCURITÉ D'APPLICATIONS AVEC UN MODULE DE SÉCURITÉ



(57) Abstract: The aim of the invention is a method for managing the security of the assembly of equipment, security module and applications. Said aim is achieved, by means of a method for managing the security of applications (APP), functioning in a piece of equipment (CB), connected to a network (NET), comprising the following preliminary steps: receipt of data comprising at least the type and the version of the equipment software (CB) and the identity of the security module (SIM), over the network by the control server, analysis and verification by the control server (CSE) of said data (ID), generation of a cryptogramme (J), from the result of the verification of said data (ID), and transmission of said cryptogramme (J), by means of the network (NET) and the equipment (CB), to the security module (SIM). Said method is characterised in that the security module (SIM) analyses the cryptogramme (J) received and activates and deactivates, respectively, resources (RES) (data or functions), used by at least one application (APP), installed in the equipment (CB).

[Suite sur la page suivante]

WO 2005/046278 A3



PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN,
TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

- (84) États désignés (*sauf indication contraire, pour tout titre de protection régionale disponible*) : ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasién (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Publiée :

- avec rapport de recherche internationale
- avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues

- (88) Date de publication du rapport de recherche internationale:

11 août 2005

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

(57) **Abrégé :** Le but de la présente invention est de proposer une méthode de gestion de la sécurité de l'ensemble équipement, module de sécurité, applications. Ce but est atteint par une méthode de gestion de la sécurité d'applications (APP) fonctionnant dans un équipement (CB) connecté à un réseau (NET), comprenant les étapes préliminaires suivantes: réception de données comprenant au moins le type et la version de logiciel de l'équipement (CB) et l'identité du module de sécurité (SIM), via le réseau, par le serveur de contrôle ; analyse et vérification par le serveur de contrôle (CSE) desdites données (ID); génération d'un cryptogramme (J) à partir du résultat de la vérification sur lesdites données (ID), et transmission dudit cryptogramme (J), via le réseau (NET) et l'équipement (CB), au module de sécurité (SIM), ladite méthode est caractérisée en ce que le module de sécurité (SIM) analyse le cryptogramme (J) reçu et active, respectivement désactive des ressources (RES) (données ou fonctions) utilisées par au moins une application (APP) installée dans l'équipement (CB).